Qwest
607 14th Street, NW, Suite 950
Washington, DC 20005
Phone 303-383-6651
Facsimile 303-896-1107

Kathryn Marie Krause
Associate General Counsel

February 27, 2009

FILED VIA ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to the Federal Communications Commission's *Report and Order*,[1] Qwest hereby files its Annual 47 C.F.R. § 64.2009(e) CPNI Certification.

Please contact me at the above-listed information if you have any questions.

/s/ Kathryn Marie Krause

cc: Best Copy and Printing, Inc. (fcc@bcpiweb.com)
Enforcement Bureau, Telecommunications Consumers Division
(two copies via courier)

---

[1] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007). *Also see*, Public Notices, DA 09-240 (Feb. 13, 2009) and DA 09-9 (Jan. 7, 2009.

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36

Annual 64.2009(e) Customer Proprietary Network Information ("CPNI") Certification for 2008

Date filed: February 27, 2009

Name of companies covered by this certification:

Form 499 Filer ID: 808440 Qwest Corporation
814711 Malheur Home Telephone Company
807684 El Paso County Telephone Company
808439 Qwest Wireless, LLC
808882 Qwest Communications Corporation (now known as Qwest Communications Company, LLC)
822734 Qwest LD Corp.

Name of signatory: Alwin Roberts

Title of signatory: Senior Vice President – Sales – Mass Markets

I, Alwin Roberts, am an officer of Qwest Corporation (a local exchange carrier). Acting as an agent of that company, and on behalf of the other companies identified above (collectively Qwest), I certify that I have personal knowledge that these companies have established operating procedures that are adequate to ensure compliance with the Federal Communications Commission's ("FCC") CPNI rules. *See* 47 C.F.R. § 64.2001, *et seq.* My personal knowledge is based, in part, on the personal knowledge of those persons who represent to me that their organizations have procedures in place to ensure compliance with the FCC's CPNI rules.

Attached to this certification is an accompanying statement (Exhibit 1) describing how the various companies have established operating procedures that are adequate to ensure compliance with the requirements set forth in section 64.2001, *et seq.* of the FCC's rules.

Actions Against Data Brokers. None of the Qwest companies identified above took action in 2008, in the courts or before regulatory bodies, against data brokers.

Customer Complaints. *Summary.* The Qwest companies identified above received 18 customer complaints in 2008 alleging the unauthorized access or release of CPNI. Qwest investigated each of these complaints. Of the 18 complaints, 12 were determined to be unfounded; 1 was never proven (customer could not be reached after numerous attempts); and 6 were reported to the Federal Bureau of Investigation ("FBI") and United States Secret Service ("USSS"), through the portal established for improper CPNI disclosures. A summary of those reported events is below.

Of the 18 allegations of unauthorized access, use or disclosure of CPNI, 3 involved allegations of improper access by Qwest employees; 11 involved allegations of improper access to **online** information to individuals not authorized to access the information;[1] and 5 involved allegations of improper disclosure of CPNI to individuals not authorized to receive it.

As noted above, 6 of the allegations were verified as involving some kind of improper access, use or disclosure of CPNI and were reported to the FBI/USSS. A summary of those incidences follows:

- 3 complaints related to ex-spouses having unauthorized online access to a customer's account.

  February 19, 2008 – a customer reported an unauthorized change in her online account user name and password; and she advised that her ex-husband and his girlfriend were harassing her and she believed they had made the changes. Qwest worked with the customer to establish a new username and password to prevent future unauthorized access.

  March 14, 2008 – a customer reported that his former spouse created and accessed an online account profile related to his service even though she was no longer authorized on his account. Qwest made some changes to its online security mechanisms that will prevent the former spouse from gaining access to the customer's account in the future.

  July 1, 2008 – A customer reported that someone, most likely his soon to be ex-wife, gained access to his online account without authorization. Qwest advised the customer to change the security question and answer for access to his online account. Qwest has received no further reports regarding this matter. Qwest made some changes to its online security mechanisms that will prevent the former spouse from gaining access to the customer's account in the future.

- 2 complaints were the result of isolated incidents in Qwest's systems, which have been resolved.

  February 19, 2008 – Qwest reported to the FBI/USSS that a customer had reported seeing another customer's unbilled wireless usage online. Qwest determined that the exposure resulted from an extremely isolated, unlikely and coincidental systems incident which had been fixed on February 8, 2008.

[1] In these figures, please note that 1 allegation is counted twice: once as an employee allegation and once as an unauthorized online disclosure.

May 2, 2008 – a new customer reported seeing another customer's billing information online. The information was viewable because the new customer had received a randomly-generated customer code that was then matched to a randomly-generated telephone number. That telephone number + customer code turned out to match information associated with an account that had been cancelled more than a year earlier. Qwest removed the old customer's billing information and began analyzing how to prevent the recurrence of this extremely unlikely coincidence.

- 1 involved an employee's improper release of CPNI.

  May 5, 2008 – a customer contacted a Qwest consultant to request information about its services. The consultant provided the information to the customer in a spreadsheet that inadvertently included information on the services of approximately 40 other Qwest small business customers. The spreadsheet did not include billing or call detail information for any customer. Qwest contacted the customer who received the spreadsheet and confirmed that it had been deleted and destroyed. Qwest worked with the employee and her manager to reinforce Qwest's policies and training on the appropriate handling of customer account information.

Signed Alwin Roberts
[Electronic Signature]

EXHIBIT 1 TO COMPLIANCE CERTIFICATE
Qwest Statement of Operating Procedures

Below, Qwest describes its operating procedures to ensure compliance with the Federal Communications Commission's ("FCC") Customer Proprietary Network Information ("CPNI") rules set forth in 47 C.F.R., Subpart U:

1. Al Roberts, Senior Vice President, Sales in Mass Markets is Qwest's CPNI Certifying Officer. Once a year, Qwest utilizes a certification process in which the managers of those business units that might use CPNI for sales or marketing certify to Mr. Roberts that, based on their personal knowledge, their business and market units have practices and procedures in place to ensure compliance with the FCC's CPNI rules.

2. Qwest also takes advantage of the expertise and experience of a variety of its other (non-sales) organizational units and personnel in addressing privacy and CPNI issues. Qwest has a Chief Privacy Officer ("CPO"), within the Risk Management organization, whose duties include advice and counsel on a variety of privacy issues. Within that Risk Management organization there is also an Information Security and Technology group, and technical CPNI issues are vetted with it. Still within that organization, Qwest has a dedicated CPNI Compliance Manager with more than a decade of experience in addressing and counseling on the proper uses of CPNI. That Compliance Manager, along with other Qwest Risk Management employees, including the CPO and the Information Security and Technology group, is responsible for assisting Qwest business units on a host of issues, including product development, training, discipline and supervision of marketing campaigns. Finally, all of the Qwest employees referenced above interact with senior Qwest legal counsel on CPNI matters that require legal analysis or advice. That counsel has been involved in CPNI issue for over 25 years. Qwest is confident that this cooperative and collaborative cross-discipline approach to CPNI issues creates an atmosphere and structure that frame and support operating procedures adequate to ensure compliance with the FCC's CPNI rules.

3. In order to ensure that CPNI issues are resolved uniformly across the business and in a timely manner, the CPNI Compliance Manager hosts bi-weekly (and if necessary weekly) CPNI conference calls which are attended by senior CPNI legal counsel. When appropriate, members of the business units, Qwest's CPO, or other Qwest attorneys will attend these calls. During these calls, CPNI issues are discussed, issues are raised, solutions are reached and/or action plans are established. In addition, the CPNI Certifying Officer is consulted or advised as necessary.

4. In addition to the management structure addressed above that is designed to appropriately address CPNI issues, all Qwest employees receive general annual training on CPNI rules. Employees with direct sales, marketing and product

responsibilities receive more-detailed training on the proper use of CPNI than the employee base generally. This detailed training includes instructions on how to recognize and properly address CPNI issues during inbound sales calls, as well as instruction on outbound marketing campaigns, including how CPNI may and may not be used during such campaigns and what administrative records must be kept. Further, on an ongoing basis, targeted training is conducted as needed.

5. Beyond its annual training, Qwest has created CPNI "methods," available for all its employees that are likely to access, use or disclose CPNI. Those methods address, for example, how Qwest employees should deal with CPNI in the context of a telephone conversation or in a Qwest sales outlet. For example, the methods advise that employees should not disclose call detail records absent special customer verification (*i.e.*, a password), *unless* the customer provides the employee with specific details about the call in question so that the employee is responding to the information given by the customer. Those methods also state that in-store employees should not release CPNI to customers unless the customer presents a valid photo ID. Qwest publishes its methods internally for easy access and consultation and uses those methods in face-to-face training sessions, as well.

6. Qwest does not allow its customers to use biographical or account information to access CPNI online. Customers not exempt from the rules (*i.e.*, certain large business customers) must authenticate themselves using a Qwest-issued security code to establish an online username and password. Additionally, Qwest has procedures regarding notifying customers when passwords, a response to a back-up means of authentication for a lost or forgotten password, online account, or address of record are created or changed.

7. Qwest sales personnel are required to obtain supervisory approval for their outbound marketing campaigns. They are required to maintain a record of their campaigns that use CPNI, including such details as: a description of the campaign (including the proposed dates and campaign purpose), the CPNI that was used and the products or services intended to be offered. The records are maintained for a minimum of one year.

8. Where Qwest expects to make CPNI available to agents or vendors, it has strong contractual provisions to protect the access, use and disclosure of CPNI, including provisions that limit the use of CPNI to those purposes for which it is provided and prohibit the improper disclosure of CPNI. These contractual provisions were renewed, updated and strengthened in 2008 to Qwest's template procurement contracts. Additionally, in those cases where an agent acts as a branded Qwest representative, Qwest provides appropriate training and scripting. In other situations, where branding is absent, the training might be more targeted to the specific task the vendor is expected to perform.

9. Qwest has a Quality Assurance Group that monitors employee calls for, among other things, compliance with the CPNI rules and correct customer authentication.

That Group provides feedback to managers for training purposes; and if appropriate, disciplinary action.

10. Qwest has documented disciplinary procedures regarding CPNI errors beyond its Quality Assurance Group. A potential violation of CPNI rules is investigated, and, where appropriate, disciplinary action is taken.

11. Qwest requires its employees to report the unauthorized access, use or disclosure of CPNI to a central point, *i.e.*, its general internal advice line, for further investigation. Customer complaints sometimes also come to Qwest's attention through that line.

12. Qwest takes reasonable measures to discover and protect against attempts to gain authorized access to CPNI. Qwest performs routine security evaluations and security assessments on Qwest systems, including those containing CPNI. Additionally, the Information Security and Technology group performs external penetration tests on Internet-facing web portals to ensure proper security is maintained. These activities further ensure that the necessary information-security safeguards are maintained with respect to CPNI and other customer information.

13. Qwest works with law enforcement regarding unauthorized access, use or disclosures of CPNI or other customer information when appropriate, even beyond the requirements of the FCC's rules. With respect to the reporting of CPNI "breaches" under the FCC-mandated process (*e.g.*, to the Department of Justice portal), Qwest has a single point-of-contact employee who does that reporting. That employee first reviews the allegations and, after investigation, if a breach warrants reporting, she does the reporting. A log of such reports is maintained and Qwest will be maintaining these records for at least two years.